

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-171504

(P2002-171504A)

(43) 公開日 平成14年6月14日 (2002.6.14)

(51) Int.Cl.⁷

識別記号

F I

テーマコード(参考)

H 0 4 N 7/167

H 0 4 H 1/00

F 5 C 0 2 5

H 0 4 H 1/00

H 0 4 N 5/455

5 C 0 6 4

H 0 4 N 5/455

7/167

Z

審査請求 未請求 請求項の数10 O L (全 10 頁)

(21) 出願番号 特願2000-366310(P2000-366310)

(22) 出願日 平成12年11月30日 (2000. 11. 30)

(71) 出願人 000003821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 田伐 智

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 内藤 康文

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100090446

弁理士 中島 司朗 (外1名)

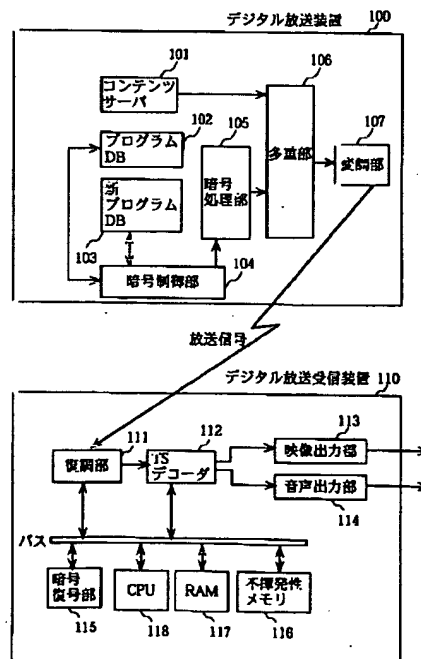
最終頁に続く

(54) 【発明の名称】 デジタル放送装置、デジタル放送受信装置及びこれらからなるデジタル放送システム並びにコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 各デジタル放送受信装置における制御プログラムを暗号化して送信するデジタル放送システムを提供する。

【解決手段】 デジタル放送装置100は、各デジタル放送受信装置110を制御するのと同じ制御プログラムをプログラムDB102に記憶し、バージョンアップした新制御プログラムを新プログラムDB103に記憶している。暗号処理部105は、新制御プログラムを制御プログラムの一部のデータを用いて暗号化する。暗号化された新制御プログラムを変調部107により多重し、送信する。デジタル放送受信装置110のTSデコーダ部112は、受信されたTSから暗号化された新制御プログラムを含むダウンロードデータを分離する。暗号復号部115は、CPU118からヘッダ情報の暗号属性に記載された不揮発性メモリ116に記憶されている制御プログラムのデータの通知を受け、復号鍵として暗号化された新制御プログラムを復号する。



【特許請求の範囲】

【請求項1】 各デジタル放送受信装置を現在制御しているのと同じ第1のプログラムを記憶している第1記憶手段と、
デジタル放送受信装置で利用される第2のプログラムを記憶している第2記憶手段と、
上記第2のプログラムを上記第1のプログラムを鍵として用いて暗号化する暗号化手段と、
暗号化された第2のプログラムをトランスポートストリームに多重化して放送する送信手段とを備えることを特徴とするデジタル放送装置。

【請求項2】 前記暗号化手段は、
暗号化した第2のプログラムに上記第1のプログラムデータのいずれの部分の暗号鍵として用いたかを暗号属性として記録したヘッダ情報を付加するヘッダ情報付加部を有することを特徴とする請求項1記載のデジタル放送装置。

【請求項3】 上記第1のプログラムは、複数のバージョンを有し、
前記ヘッダ情報付加部は、バージョンごとの暗号属性を記録することを特徴とする請求項2記載のデジタル放送装置。

【請求項4】 第1のプログラムを鍵として用いて暗号化された第2のプログラムを多重化したトランスポートストリームを受信するデジタル放送受信装置であって上記第1のプログラムを記憶している記憶手段と、
受信したトランスポートストリームから暗号化された第2のプログラムを分離する分離手段と、
分離された暗号化された第2のプログラムを第1のプログラムを鍵として用いて復号する復号手段とを備えることを特徴とするデジタル放送受信装置。

【請求項5】 上記暗号化された第2のプログラムには、第1のプログラムデータのいずれの部分の暗号鍵として用いたかを暗号属性として記録したヘッダ情報が付加されており、

前記復号手段は、
前記記憶手段に記憶されている第1のプログラムデータから暗号属性に記録された部分のデータを読み出し復号鍵を取得する復号鍵取得部と、
取得した復号鍵で暗号化された第2のプログラムを復号する復号処理部とを有することを特徴とする請求項4記載のデジタル放送受信装置。

【請求項6】 上記ヘッダ情報には、更に、デジタル放送受信装置を識別する固有IDが含まれており、
前記分離手段は、付加されたヘッダ情報に含まれる固有IDが自装置のそれと一致する暗号化された第2のプログラムを分離することを特徴とする請求項5記載のデジタル放送受信装置。

【請求項7】 上記第1のプログラムは、現在動作中の制御プログラムであり、

上記第2のプログラムは、上記制御プログラムをバージョンアップしたものであり、

前記復号手段で復号されたプログラムが正常であるかを判定し、正常であると判定したとき、復号されたプログラムを前記記憶手段に記憶されている第1のプログラムと置き換える置換手段を更に備えることを特徴とする請求項4、5又は6に記載のデジタル放送受信装置。

【請求項8】 請求項4、5又は6記載のデジタル放送受信装置は、更に外部機器に接続された外部機器制御手段を備え、

前記外部機器制御手段は、前記復号手段で復号された第2のプログラムが正常であるとき、前記外部機器に出力し、

前記外部機器は、出力された第2のプログラムで制御されることを特徴とするデジタル放送受信装置。

【請求項9】 デジタル放送装置と、該装置から放送されるトランスポートストリームを受信する複数のデジタル放送受信装置とからなるデジタル放送システムであって、

前記デジタル放送装置は、
各デジタル放送受信装置を現在制御しているのと同じ第1のプログラムを記憶している第1記憶手段と、
デジタル放送受信装置で利用される第2のプログラムを記憶している第2記憶手段と、

上記第2のプログラムを上記第1のプログラムを鍵として用いて暗号化する暗号化手段と、

暗号化された第2のプログラムをトランスポートストリームに多重化して放送する送信手段とを備え、

前記各デジタル放送受信装置は

上記第1のプログラムを記憶しているプログラム記憶手段と、

受信されたトランスポートストリームから暗号化された第2のプログラムを分離する分離手段と、

分離された暗号化された第2のプログラムを上記第1のプログラムを鍵として用いて復号する復号手段とを備えることを特徴とするデジタル放送システム。

【請求項10】 第1のプログラムを記憶し、第1のプログラムで制御され、第1のプログラムを鍵として用いて暗号化された第2のプログラムを多重化したトランスポートストリームを受信するデジタル放送受信装置に適用されるコンピュータ読み取り可能な記録媒体であって、

受信したトランスポートストリームから暗号化された第2のプログラムを分離する分離手段と、

分離された暗号化された第2のプログラムを第1のプログラムを鍵として用いて復号する復号手段との各手段の機能をコンピュータに発揮させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はデジタル放送において、プログラムデータを安全に送受信するデジタル放送装置及びデジタル放送受信装置並びにこれらからなるデジタル放送システムに関する。

【0002】

【従来の技術】現在ほとんどのデジタル放送で用いられているMPEG2規格では、映像、音声等はそれぞれの規定に従ってパケット化された後、トランスポートストリーム上に時分割多重され、受信装置に送信される。各受信装置では、受信したトランスポートストリームより、必要な映像、音声等のパケットを分離し、復号を行っている。

【0003】ところで、近年デジタル放送においてはサービスが多様化し、映像や音声だけでなくデータ放送等も行われてきている。多様化するサービスを実現するために、受信装置はサービスが追加あるいは変更される毎に、そのサービスに対応できる動作プログラムに更新することが必要であり、かつこのような変更リアルタイムに対応することが要求されている。この要求を満足するために、最近のデジタル放送システムは、受信装置の動作を制御する制御プログラムを放送装置から送出し、受信装置では、その制御プログラムを受信して自動的に新しい制御プログラムで動作することが可能となる制御プログラム更新機能を有しており、例えば特開平11-4451号公報に記載されたものがある。

【0004】従来の制御プログラム更新方法について、図9を用いて説明する。図9は、デジタル放送システムにおける従来の放送受信装置の構成図である。放送受信装置において、放送装置から送信された放送信号は、復調部901に入力され、復調処理を施され、トランスポートストリームのビット列としてTS(トランスポートストリーム)デコーダ902に入力される。TSデコーダ902は、入力されたトランスポートストリームから、必要なパケットを選択・分離し、映像パケットを映像出力部903に、音声パケットを音声出力部904に、データパケットをCPU905にそれぞれ出力する。映像出力部903は、TSデコーダ902から入力された映像パケットを一般のTV受像機やモニタに表示できるような信号に変換を行う。音声出力部904は、TSデコーダ902から入力された音声パケットをアナログ音声信号に変換し、スピーカに出力する。

【0005】CPU905は、通常フラッシュメモリ等の不揮発性メモリ906に記憶された制御プログラムに従って制御動作を行っている。例えば、ユーザインターフェース部907からの入力に従って、TSデコーダ902に対して選択する番組チャンネルの指示動作等を行い、TSデコーダ902から入力されたデータパケットが番組表等の付加サービス情報である場合には、その情報に従って制御動作を行う。ただし、入力されたデータパケットが新しい制御プログラムである場合には、一旦

RAM908に保存し、データが正常か否かを判断した後、正常であれば現在動作中の制御プログラムを削除し、新しい制御プログラムを不揮発性メモリ906に書き込む。以上の動作が正常に終了した後、CPU905は、リセット回路909にリセット指示を行い、放送受信装置は書き換えられた新しい制御プログラムで動作を開始する。これによって、放送受信装置はサービスの追加や変更リアルタイムに対応するようにしている。

【0006】

【発明が解決しようとする課題】ところで、放送装置からプログラムデータを各放送受信装置に送出する場合には、広範囲にプログラムデータが流れることになるため、関係のない第三者も簡単にプログラムデータを取得できる。そのため、プログラムデータの情報漏洩や改ざん等が容易に行えるため、何らかの方法でセキュリティを確保することが望まれる。

【0007】しかしながら、従来のプログラム更新方法では、放送装置から送られてくるプログラムに対して特にセキュリティは考えられていないのが現状である。また、何らかの方法でプログラムにセキュリティ機能が設けられている場合でも、放送受信装置にはそのセキュリティを解除するためのデータをあらかじめ保存しておく必要があり、そのデータを容易に変更できないため、セキュリティ方法が単純化するという問題点がある。

【0008】本発明は、このような課題を解決し、放送装置から送出するプログラムデータの秘匿性を高めることができ、かつその方法が単純化しないようにしたデジタル放送システムを提供することを目的としている。

【0009】

【課題を解決するための手段】本発明は、上記目的を達成するためデジタル放送装置と、該装置から放送されるトランスポートストリームを受信する複数のデジタル放送受信装置とからなるデジタル放送システムであって、前記デジタル放送装置は、各デジタル放送受信装置を現在制御しているのと同じ第1のプログラムを記憶している第1記憶手段と、デジタル放送受信装置で利用される第2のプログラムを記憶している第2記憶手段と、上記第2のプログラムを上記第1のプログラムを鍵として用いて暗号化する暗号化手段と、暗号化された第2のプログラムをトランスポートストリームに多重化して放送する送信手段とを備え、前記各デジタル放送受信装置は上記第1のプログラムを記憶しているプログラム記憶手段と、受信されたトランスポートストリームから暗号化された第2のプログラムを分離する分離手段と、分離された暗号化された第2のプログラムを上記第1のプログラムを鍵として用いて復号する復号手段とを備えることとしている。

【0010】

【発明の実施の形態】以下、本発明に係るデジタル放送システムの実施の形態について図面を用いて説明する。

(実施の形態1) 図1は、本発明に係るデジタル放送システムの実施の形態1の構成図である。デジタル放送システムは、放送信号を送出するデジタル放送装置100と放送信号を受信する複数のデジタル放送受信装置110とから構成される。

【0011】デジタル放送装置100は、コンテンツサーバ101と、プログラムDB(データベース)102と、新プログラムDB103と、暗号制御部104と、暗号処理部105と、多重部106と、変調部107とを備えている。各デジタル放送受信装置110は、復調部111と、TSデコーダ112と、映像処理部113と、音声処理部114と、暗号復号部115と、不揮発性メモリ116と、RAM117と、CPU118とを備えている。

【0012】コンテンツサーバ101は、1以上のコンテンツを記憶しており、コンテンツをMPEG(Moving Picture Experts Group)2規格のトランスポートストリームパケットの形式で多重部106に通知する。ここで、コンテンツは、各チャネルで放送される番組であり、映像データや音声データを含んでいる。更に、コンテンツサーバ101は、トランスポートストリームを受信するデジタル放送受信装置110における番組選択に必要な情報である番組配列情報(PSI: Program Specific Information)を併せて多重部106に通知する。

【0013】プログラムDB102は、各デジタル放送受信装置110で、現在動作中の制御プログラムを管理している。なお、各デジタル放送受信装置110で動作中の制御プログラムは、デジタル放送受信装置のメーカーや機種により異なる場合があり、また、同一メーカーの同一機種であっても使用しているバージョンが異なる場合もある。したがって、プログラムDB102には、通常、複数種類の制御プログラムが管理されている。

【0014】各制御プログラムは、制御プログラムの本体データと、制御プログラムが適用されているデジタル放送受信装置110のメーカー名や機種を識別する固有IDと、制御プログラムのバージョン番号とで構成されている。新プログラムDB103は、各デジタル放送受信装置110で現在動作中の制御プログラムに換えて、新しく制御プログラムとして利用されるバージョンアップされた制御プログラム(以下「新制御プログラム」という)を管理している。この新制御プログラムは、所定の期間、デジタル放送装置100から各デジタル放送受信装置110に送出され、適合するデジタル放送受信装置110で現在の制御プログラムと置き換えられた後は、暗号制御部104によって、プログラムDB102に書き移される。

【0015】この新制御プログラムも動作中のプログラムと同様、制御プログラムのデータ本体と、固有IDと、バージョン番号とから構成されている。暗号制御部

104は、顧客管理情報と暗号化条件とを記憶し、暗号処理部105を制御する。顧客管理情報は、デジタル放送を受信するユーザごとにユーザIDと、デジタル放送受信装置110の固有IDと、そのデジタル放送装置110での暗号化方法とが記載されている。

【0016】暗号化条件には、複数の暗号方法が記載されており、使用されるデジタル放送装置110のたとえばメーカーや機種ごとの固有IDに対応した暗号化の方法を定めている。暗号制御部104は、図示しない指示部から新制御プログラムの送出指示を受けると、新プログラムDB103に記憶されている新制御プログラムを読み出す。読み出した新制御プログラムの固有IDに対応した暗号化の方法を暗号化条件より選択し、暗号処理部105に通知する。

【0017】更に、暗号制御部104は選択した暗号化の方法に従い、新制御プログラムの固有IDの一致し、かつ新制御プログラムのバージョン番号の1つ前のバージョン番号の制御プログラムをプログラムDB102から読み出し、新制御プログラムとともに暗号処理部105に通知する。暗号処理部105は、暗号制御部104から通知された暗号化の方法に従い、新制御プログラムのデータ本体を暗号化する。

【0018】暗号処理部105は、暗号制御部104から暗号化の方法とともに、新制御プログラムと新制御プログラムに対応する現在デジタル放送受信装置110で動作中の制御プログラム(以下「動作中制御プログラム」という)とを通知されている。図2は、暗号処理部105での暗号化処理の状態を説明する模式図である。暗号処理部105は、暗号化の方法に従い、動作中制御プログラムのデータ本体201の一部を暗号鍵202として、新制御プログラムのデータ本体203を暗号化処理(スクランブル)し、新制御プログラムの暗号化されたデータ本体204を生成する。

【0019】ここで、暗号鍵202は、データ本体201の一部のデータを用いており、暗号化処理は、予め決められた暗号方式、例えば、新制御プログラムのデータ本体203と暗号鍵202との排他的論理和を求めることにより、暗号化された新プログラムのデータ本体204が生成される。暗号処理部105は、図3に示すように、生成した暗号化された新プログラムのデータ本体204に、バージョン番号301と固有のID302と現バージョン番号303と暗号属性304とをヘッダ情報として付加したダウンロードデータ305を多重部106に通知する。ここで、バージョン番号301は新制御プログラムのバージョン番号であり、固有ID302は新制御プログラムと動作中制御プログラムとに共通する特定のデジタル放送受信装置110のメーカー名や機種名を示す識別子であり、現バージョン番号303は動作中制御プログラムのバージョン番号であり、暗号属性304は暗号鍵202とされる動作中制御プログラムのデー

タ本体201の位置情報であるアドレスを示している。

【0020】多重部106は、コンテンツサーバ101から通知されたコンテンツのトランスポートストリームパケットと番組配列情報とを併せて、暗号処理部105から通知されたダウンロードデータ305をトランスポートストリームに多重化して変調部107に通知する。変調部107は、多重部106から通知されたトランスポートストリームを放送信号に変調して各デジタル放送受信装置110に送出する。

【0021】次に、デジタル放送受信装置110について説明する。復調部111は、CPU118の制御に従い、デジタル放送装置100から送出される放送信号を受信復調して、トランスポートストリームをTSデコーダ112に通知する。TSデコーダ112は、CPU118の制御に従い、通知されたトランスポートストリームから、映像パケットを分離し映像出力部113に通知し、音声パケットを分離し音声出力部114に通知し、番組配列情報パケットを分離しRAM117に書き込み、ダウンロードデータ305のパケットを分離しRAM117に書き込み、併せてCPU118に通知する。

【0022】映像出力部113は、TSデコーダ112から通知された映像パケットを外部のモニタに表示できる信号に変換して出力する。音声出力部114は、TSデコーダ112から通知された音声パケットをアナログ音声信号に変換し、外部スピーカに出力する。暗号復号部115は、CPU118から復号鍵の通知を受けると、予め記憶している復号方法により、RAM117に記憶されている暗号化されている新制御プログラムのデータ本体を読み出し、復号鍵を用いて復号化（デスクランブル）する。例えば、復号方法が排他的論理和の計算であれば、暗号化されている新制御プログラムと復号鍵との排他的論理和を計算し、復号化する。復号化された新制御プログラムをRAM117に書き込む。

【0023】図4は、暗号復号部115での復号化処理を説明する模式図である。暗号化された新制御プログラムのデータ本体204は、CPU118によってRAM117に書き込まれている。動作中制御プログラムのデータ本体201は、不揮発性メモリ116に記憶されている。暗号復号部115は、この動作中制御プログラムのデータ本体201の一部のデータを復号鍵401として、CPU118から通知される。暗号復号部115は、通知された復号鍵401を用いて暗号化された新制御プログラムのデータ本体を記憶している復号方法により復号処理し、復号した新制御プログラムのデータ本体203をRAM117に書き込み、復号の終了をCPU118に通知する。

【0024】なお、復号鍵401は、デジタル放送装置100において、暗号処理部105で暗号鍵202として用いられたデータと同一である。不揮発性メモリ116は、フラッシュROM等からなり、デジタル放送受信

装置110の各部を制御する制御プログラムが記憶されている。CPU118は、この制御プログラムに従い各部を制御する。不揮発性メモリ116には、現在動作中制御プログラムのデータ本体201がバージョン番号とともに記憶されている。バージョンアップされた新制御プログラムのデータ本体203がRAM117に書き込まれ、CPU118が新制御プログラムが正しいことを確認した後、動作中制御プログラムに換えて新制御プログラムが不揮発性メモリ116に記憶される。

【0025】RAM117は、CPU118のワークエリアとして構成され、TSデコーダ112で分離された番組配列情報が書き込まれ、またTSデコーダ112で分離されたダウンロードデータ305が書き込まれる。また、RAM117には、ダウンロードデータ305に含まれる暗号化された新制御プログラムのデータ本体204の復号化された新制御プログラムのデータ本体203が暗号復号部115によって書き込まれる。

【0026】CPU118は、不揮発性メモリ116に記憶されている動作中制御プログラムに従い、各部を制御する。CPU118は、TSデコーダ112によって、1つ以上のダウンロードデータ305が分離され、RAM117に書き込まれると、ヘッダ情報の固有ID302が自装置110の固有IDと一致するダウンロードデータの有無を判定し、無いと判定したときは、TSデコーダ112に更に適合するダウンロードデータ305を分離するよう指示する。また、一致しているときは、バージョン番号301が不揮発性メモリ116に記憶されている動作中制御プログラムのバージョン番号を更新したものであるか否かを判定する。否のときは、TSデコーダ112に更に適合するダウンロードデータ305を分離するよう指示し、RAM117のダウンロードデータ305を消去する。肯定の時は、RAM117に記録されたダウンロードデータ305の暗号属性304を読み出す。暗号属性304に記載されたアドレスに従い、不揮発性メモリ116に記憶されている動作中制御プログラムの一部データを復号鍵として取得し、暗号復号部115に通知する。

【0027】CPU118は、暗号復号部115から新制御プログラムの復号を終了した旨の通知を受けると、RAM117に記憶されている新制御プログラムのデータ本体が正常か否かを判定し、正常であれば、不揮発性メモリ116に現在記憶されている動作中制御プログラムに換えて、新制御プログラムを転記する。この後、デジタル放送受信装置110は、このバージョンアップされた新制御プログラムによって制御される。

【0028】次に、デジタル放送受信装置110の暗号化された新制御プログラムの復号動作について図5のフローチャートを用いて説明する。まず、TSデコーダ112はダウンロードデータ305をトランスポートストリームから分離してRAM117に書き込む。CPU1

18は、ダウンロードデータ305のヘッダ情報の固有ID302が自装置の固有IDに一致するか否かを判定し、一致しなければ一致する固有IDのダウンロードデータ305の分離を待つ(S502)。

【0029】次に、CPU118は、ヘッダ情報のバージョン番号301が不揮発性メモリ116に記憶されているバージョン番号の更新されたものであるか否かを判定し(S504)、否であれば、S502に戻る。CPU118は、肯定のときは、ダウンロードデータ305を取得し(S506)、ヘッダ情報の暗号属性304を読み出し、不揮発性メモリ116に記憶されている動作中制御プログラムの一部データを読み出した暗号属性304に従い、復号鍵401として取得する。取得した復号鍵401を暗号復号部115に通知する(S508)。

【0030】暗号復号部115は、通知された復号鍵401を用いて、RAM117に記憶されている暗号化された新制御プログラムのデータ本体204を復号し、復号した新制御プログラムのデータ本体203を生成する。CPU118は、新制御プログラムのデータ本体203が正常か否かを判定し、正常なときは、RAM117に記憶されている新制御プログラムを不揮発性メモリ116に転記し、動作中制御プログラムと置換する(S510)。

【0031】これによって、制御プログラムのバージョンが更新される。以後、この新制御プログラムで制御される。このように、現在動作中の制御プログラムの一部のデータを復号鍵(暗号鍵)として復号化(暗号化)することによって、デジタル放送受信装置110にデジタル放送装置100から別途鍵情報を送出する必要がないと同時に、秘匿性の高いデータ送信をすることができる。

【0032】なお、本実施の形態では、暗号鍵202(復号鍵401)を動作中制御プログラムのデータ本体201の一部データを用いたけれども、全部を用いてもよいし、後述するように不連続な一部の部分を集合して用いてもよい。また、固有ID302をヘッダ情報に含めたけれども、固有ID302も暗号化する新制御プログラムのデータ本体に含めてもよい。

【0033】また、デジタル放送装置100とデジタル放送受信装置110とがケーブルで接続されたCATV等の場合には、上記ヘッダ情報にバージョン番号301、固有ID302、現バージョン番号303を含めることなく、全てのデジタル放送受信装置110に暗号化された新制御プログラムのデータ本体を送出するようにしてもよい。

【0034】また、暗号化方式については、排他的論理和の例を示したが、その他のアルゴリズムを用いることもできる。また、ダウンロードデータ305を公衆回線等の別のメディアで伝送してもよいし、又、デジタル放

送装置100が衛星等からの放送を中継するCATV等の場合には、OoB(Out-Of-BAND)と呼ばれる映像・音声とは異なる周波数帯域で送出することもできる。

【0035】また、上記実施の形態では、デジタル放送受信装置110で暗号化された新制御プログラムの復号方法を予め暗号復号部115が記憶しているようにしたけれども、ダウンロードデータ305のヘッダ情報の暗号属性304に復号方法を記載して送出するようにしてもよい。

(変形例) この変形例は、暗号鍵を動作中制御プログラムの不連続な一部のデータの集合とするものである。また、この変形例では、複数のデジタル放送受信装置110において、動作中制御プログラムに異なるバージョンの制御プログラムが用いられている場合が想定されている。

【0036】図6に示すように、各デジタル放送受信装置110では、バージョン1の制御プログラム601とバージョン2の制御プログラム602とが動作中である。制御プログラム601の位置情報「10」、「8」、「100」、「256」で示される各データ「F」、「E」、「0」、「1」を暗号鍵603とする。制御プログラム602の位置情報「150」、「65」、「60」、「3」で示される各データ「F」、「E」、「0」、「1」を同様に暗号鍵603とする。

【0037】暗号処理部105は、この暗号鍵603を用いてバージョン3の制御プログラム604を暗号化処理し、バージョン3の暗号化された制御プログラム605を生成する。図7は、暗号処理部105で生成されたダウンロードデータ700を示している。ダウンロードデータには、暗号化されたバージョン3の制御プログラム605とそのヘッダ情報として、バージョン番号701と固有ID702と暗号属性703とが含まれている。

【0038】暗号属性703には、暗号鍵603を示す動作中制御プログラム601、602のそれぞれの位置情報704、705が含まれている。デジタル放送装置100からこのダウンロードデータ700がトランスポートストリームに多重化され、デジタル放送受信装置110に送信される。デジタル放送受信装置の暗号復号部115では、不揮発性メモリ116にバージョン1の制御プログラム601が記憶されているときには、復号鍵として暗号属性703のバージョン1の位置情報704が用いられる。同様に不揮発性メモリ116にバージョン2の制御プログラム602が記憶されているときには、復号鍵として暗号属性703のバージョン2の位置情報704が用いられる。

【0039】(実施の形態2) 図8は、本発明に係るデジタル放送受信装置の実施の形態2の構成図である。このデジタル放送受信装置は、復調部111と、TSデコ

ーダ112と、映像出力部113と、音声出力部114と、暗号復号部115と、不揮発性メモリ116と、RAM117と、CPU802と、外部機器制御部803とを備え、外部機器制御部803は、外部機器804と接続されている。なお、上記実施の形態1の構成と同様の構成部分には同一の符号を付しその説明を省略し、本実施の形態固有の構成について説明する。

【0040】本実施の形態では、デジタル放送受信装置801が受信するトランスポートストリームには、デジタル放送受信装置801に接続された外部機器で利用される暗号化された制御プログラムがダウンロードデータとして多重化されている。ダウンロードデータのヘッダ情報には、バージョン番号301(図3参照)に換えて、外部機器804の固有IDが記載されている。

【0041】CPU802は、ダウンロードデータのヘッダ情報に外部機器制御部803に接続された外部機器804の固有IDが記載されているときも、上記実施の形態と同様、暗号復号部115に暗号鍵を通知し、暗号化された制御プログラムを復号して、復号化された制御プログラムを生成させる。CPU802は、生成された制御プログラムをRAM117から読み出し、外部機器制御部803に通知する。

【0042】外部機器制御部803は、例えばIEEE1394等のインターフェイスを介して外部機器804に接続されている。外部機器制御部803は、CPU802から通知された制御プログラムを外部機器804に出力する。外部機器804は、外部機器制御部803から出力された制御プログラムの入力を受け、自身の制御プログラムを更新する。なお、この外部機器804は、例えば、ゲーム機器であり、入力された制御プログラムに従いゲームを展開する。また、この外部機器804がステレオ装置であれば、入力された制御プログラムにより動作するカラオケ装置を実現する。

【0043】なお、外部機器制御部803は、IEEE1394により外部機器804と接続されたとしたけれども、他の接続方式が用いられてよいのは勿論である。また、本実施の形態では、外部機器804に復号された制御プログラムを出力するようにしたけれども、暗号化された状態で出力し、外部機器804で復号するようにしてもよい。この場合には、暗号属性に外部機器804で現在動作中の制御プログラムの一部データを用いた暗号鍵を利用する等を記載し、ダウンロードデータ全体を外部機器804に出力するようにする。

【0044】また、デジタル放送受信装置801により制御プログラムを復号し、別の暗号方式で暗号化し、外部機器804に出力するようにしてもよい。更に、上記各実施の形態では、その構成を図1と図8に示したけれども、各構成部分の機能をコンピュータに発揮させるプログラムをコンピュータ読み取り可能な記録媒体に記録しておき、このような動作中制御プログラムを用いた暗

号鍵(復号鍵)によって新制御プログラムを暗号化(復号化)する機能のないデジタル放送システムに適用し、本発明と同様の効果を発揮させることができる。

【0045】

【発明の効果】以上説明したように、本発明は、各デジタル放送受信装置を現在制御しているのと同じ第1のプログラムを記憶している第1記憶手段と、デジタル放送受信装置で利用される第2のプログラムを記憶している第2記憶手段と、上記第2のプログラムを上記第1のプログラムを鍵として用いて暗号化する暗号化手段と、暗号化された第2のプログラムをトランスポートストリームに多重化して放送する送信手段とを備えることとしている。このような構成によって、暗号化された第2のプログラムを送信する際に、同時に暗号鍵を送信する必要がなく、かつデジタル放送受信装置ごとに秘匿性の高めた第2のプログラムを送信することができる。

【0046】また、前記暗号化手段は、暗号化した第2のプログラムに上記第1のプログラムデータのいずれの部分暗号鍵として用いたかを暗号属性として記録したヘッダ情報を付加するヘッダ情報付加部を有することとしている。このような構成によって、送信先のデジタル放送受信装置に記憶されている第1のプログラムの部分データを用いて暗号化できるので、秘匿性を高めることができる。

【0047】また、上記第1のプログラムは、複数のバージョンを有し、前記ヘッダ情報付加部は、バージョンごとの暗号属性を記録することとしている。このような構成によって、各デジタル放送受信装置が異なるバージョンの第1のプログラムで制御されているときであっても、暗号化された第2のプログラムを各デジタル放送受信装置で復号化することができる。

【0048】また、本発明は、第1のプログラムを鍵として用いて暗号化された第2のプログラムを多重化したトランスポートストリームを受信するデジタル放送受信装置であって上記第1のプログラムを記憶している記憶手段と、受信したトランスポートストリームから暗号化された第2のプログラムを分離する分離手段と、分離された暗号化された第2のプログラムを第1のプログラムを鍵として用いて復号する復号手段とを備えることとしている。このような構成によって、秘匿性を高めて送信されてくる第2のプログラムを容易に復号することができる。

【0049】また、上記暗号化された第2のプログラムには、第1のプログラムデータのいずれの部分暗号鍵として用いたかを暗号属性として記録したヘッダ情報が付加されており、前記復号手段は前記記憶手段に記憶されている第1のプログラムデータから暗号属性に記録された部分のデータを読み出し復号鍵を取得する復号鍵取得部と、取得した復号鍵で暗号化された第2のプログラムを復号する復号処理部とを有することとしている。こ

のような構成によって、デジタル放送受信装置自身に記憶されているデータを用いて暗号化された第2のプログラムを容易に復号することができる。

【0050】また、上記ヘッダ情報には、更に、デジタル放送受信装置を識別する固有IDが含まれており、前記分離手段は、付加されたヘッダ情報に含まれる固有IDが自装置のそれと一致する暗号化された第2のプログラムを分離することとしている。このような構成によって、デジタル放送受信装置に適合した第2のプログラムを秘匿性の高い状態で取得することができる。

【0051】また、上記第1のプログラムは、現在動作中の制御プログラムであり、上記第2のプログラムは、上記制御プログラムをバージョンアップしたものであり、前記復号手段で復号されたプログラムが正常であるか否かを判定し、正常であると判定したとき、復号されたプログラムを前記記憶手段に記憶されている第1のプログラムと置き換える置換手段を更に備えることとしている。このような構成によって、暗号化された第2のプログラムを復号して、現在作動中の制御プログラムと置換することができる。

【0052】また、請求項4、5又は6記載のデジタル放送受信装置は、更に外部機器に接続された外部機器制御手段を備え、前記外部機器制御手段は、前記復号手段で復号された第2のプログラムが正常であるとき、前記外部機器に出力し、前記外部機器は、出力された第2のプログラムで制御されることとしている。このような構成によって、デジタル放送受信装置に接続された外部機器を制御する第2のプログラムを秘匿性の高い状態で取得することができる。

【0053】また、本発明は、デジタル放送装置と、該装置から放送されるトランスポートストリームを受信する複数のデジタル放送受信装置とからなるデジタル放送システムであって、前記デジタル放送装置は、各デジタル放送受信装置を現在制御しているのと同じ第1のプログラムを記憶している第1記憶手段と、デジタル放送受信装置で利用される第2のプログラムを記憶している第2記憶手段と、上記第2のプログラムを上記第1のプログラムを鍵として用いて暗号化する暗号化手段と、暗号化された第2のプログラムをトランスポートストリームに多重化して放送する送信手段とを備え、前記各デジタル放送受信装置は上記第1のプログラムを記憶しているプログラム記憶手段と、受信されたトランスポートストリームから暗号化された第2のプログラムを分離する分離手段と、分離された暗号化された第2のプログラムを上記第1のプログラムを鍵として用いて復号する復号手段とを備えることとしている。このような構成によって、デジタル放送装置からデジタル放送受信装置に暗号鍵を同時に送信することなく、秘匿性の高いプログラムを容易に送受信するデジタル放送システムを得ることができる。

【0054】また、本発明は、第1のプログラムを記憶し、第1のプログラムで制御され、第1のプログラムを鍵として用いて暗号化された第2のプログラムを多重化したトランスポートストリームを受信するデジタル放送受信装置に適用されるコンピュータ読み取り可能な記録媒体であって、受信したトランスポートストリームから暗号化された第2のプログラムを分離する分離手段と、分離された暗号化された第2のプログラムを第1のプログラムを鍵として用いて復号する復号手段との各手段の機能をコンピュータに発揮させるプログラムを記録したコンピュータ読み取り可能な記録媒体としている。このような構成によって、自装置を制御する第1のプログラムを用いて暗号化された第2のプログラムを復号する機能を有しないデジタル放送受信装置にこの記録媒体を適用してこのような機能を発揮させることができる。

【図面の簡単な説明】

【図1】本発明に係るデジタル放送システムの実施の形態1の構成図である。

【図2】上記実施の形態の暗号処理部における新制御プログラムの暗号化処理を説明する模式図である。

【図3】上記実施の形態の暗号処理部で生成されるダウンロードデータの構造を示す図である。

【図4】上記実施の形態の暗号復号部における復号化処理を説明する模式図である。

【図5】上記実施の形態のデジタル放送受信装置における新制御プログラムの復号動作を説明するフローチャートである。

【図6】上記実施の形態の変形例の暗号化処理を説明する模式図である。

【図7】上記変形例の暗号処理部で生成されるダウンロードデータの構造を示す図である。

【図8】本発明に係るデジタル放送受信装置の実施の形態2の構成図である。

【図9】従来の放送受信装置の構成図である。

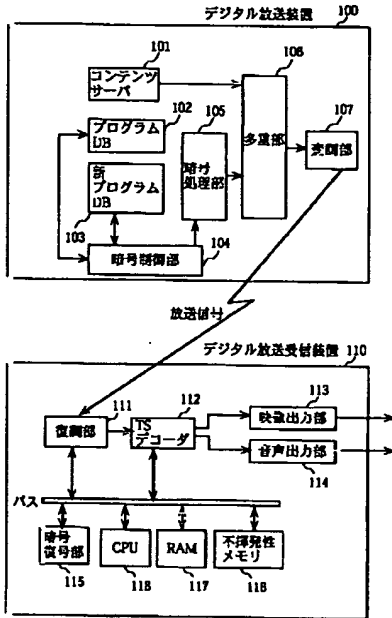
【符号の説明】

- 100 デジタル放送装置
- 101 コンテンツサーバ
- 102 プログラムDB
- 103 新プログラムDB
- 104 暗号制御部
- 105 暗号処理部
- 106 多重部
- 107 変調部
- 110, 801 デジタル放送受信装置
- 111 復調部
- 112 TSデコーダ
- 113 映像出力部
- 114 音声出力部
- 115 暗号復号部
- 116 不揮発性メモリ

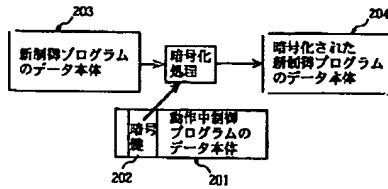
117 RAM
118.802 CPU

803 外部機器制御部
804 外部機器

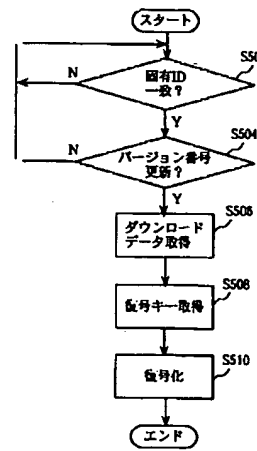
【図1】



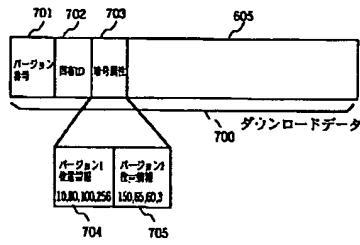
【図2】



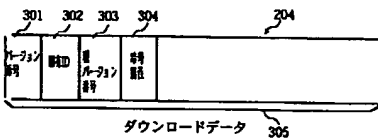
【図5】



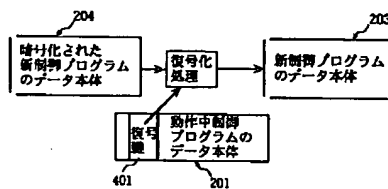
【図7】



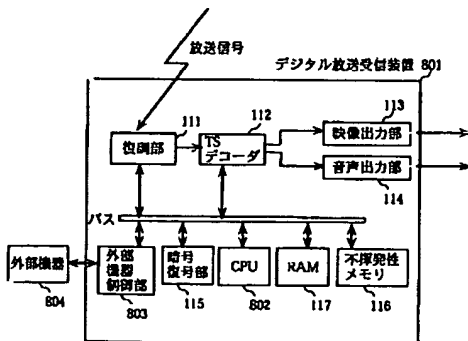
【図3】



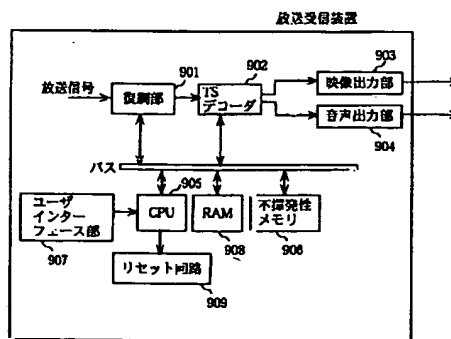
【図4】



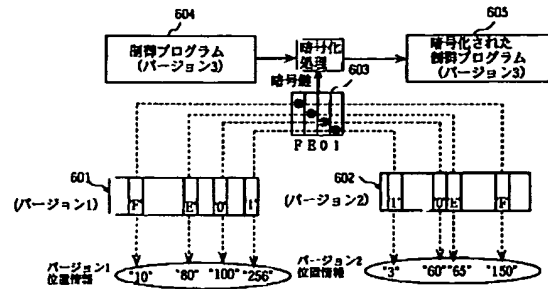
【図8】



【図9】



【図6】



フロントページの続き

(72)発明者 北 輝秀
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(72)発明者 加治 充
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 粗野 恒雄
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
Fターム(参考) 5C025 AA30 BA25 BA27 DA01
5C064 CA14 CB01 CC04